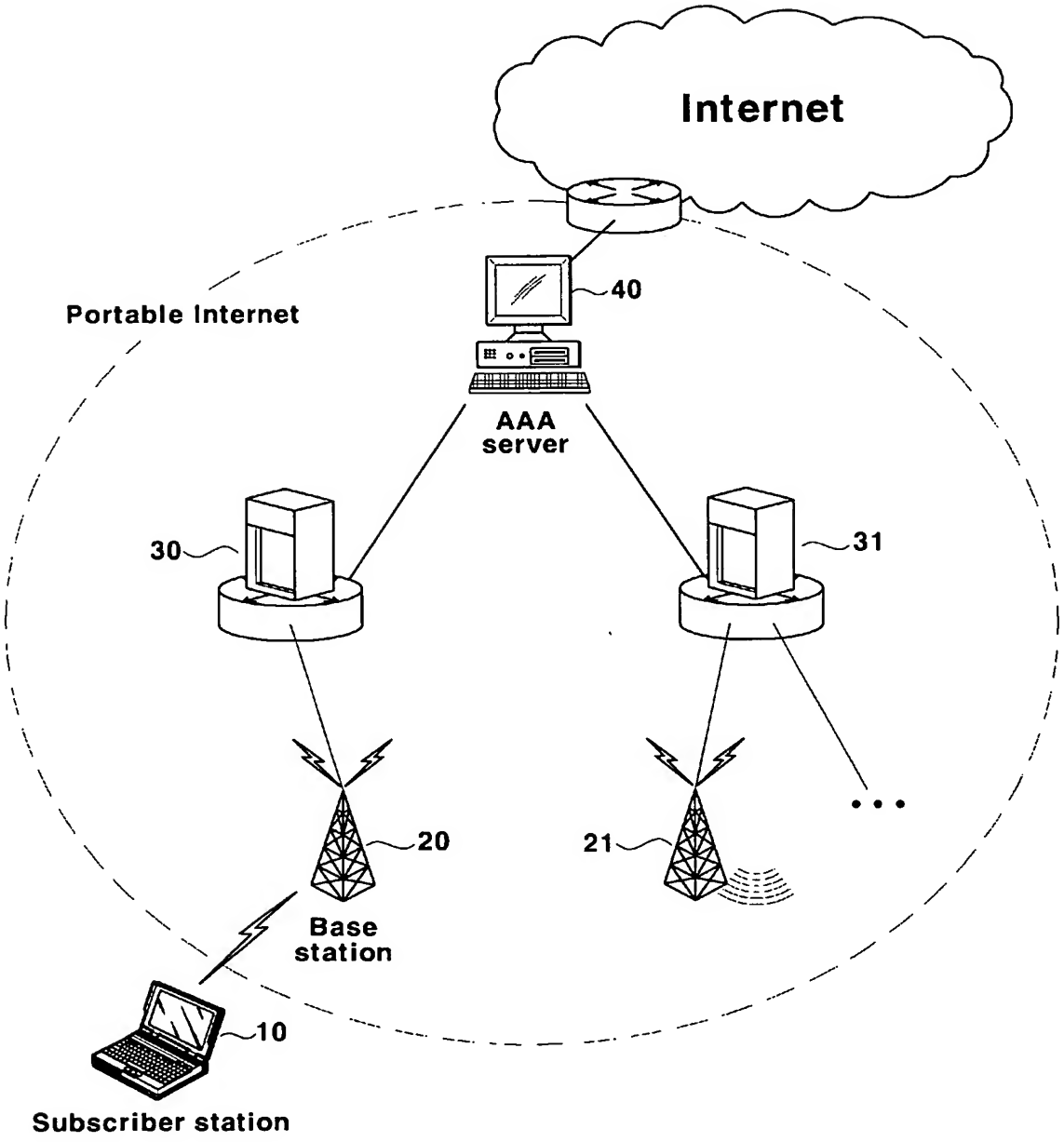
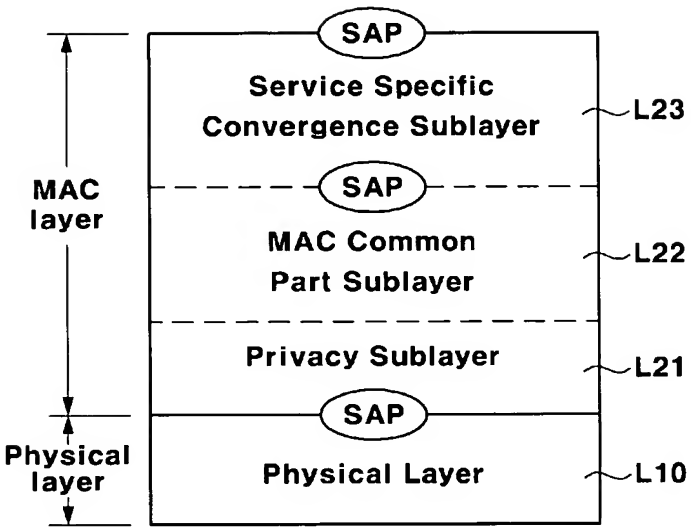
[Fig. 1]

FIG.1


Internet
Portable Internet
40
AAA server
30
31
20
21
Base station
10
Subscriber station

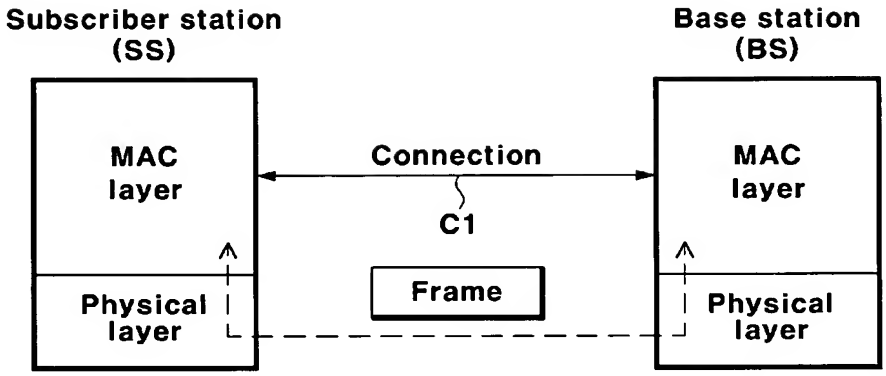
[Fig. 2]

FIG.2


SAP
Service Specific
Convergence Sublayer
L23
SAP
MAC Common
Part Sublayer
L22
Privacy Sublayer
L21
SAP
Physical Layer
L10
MAC
layer
Physical
layer

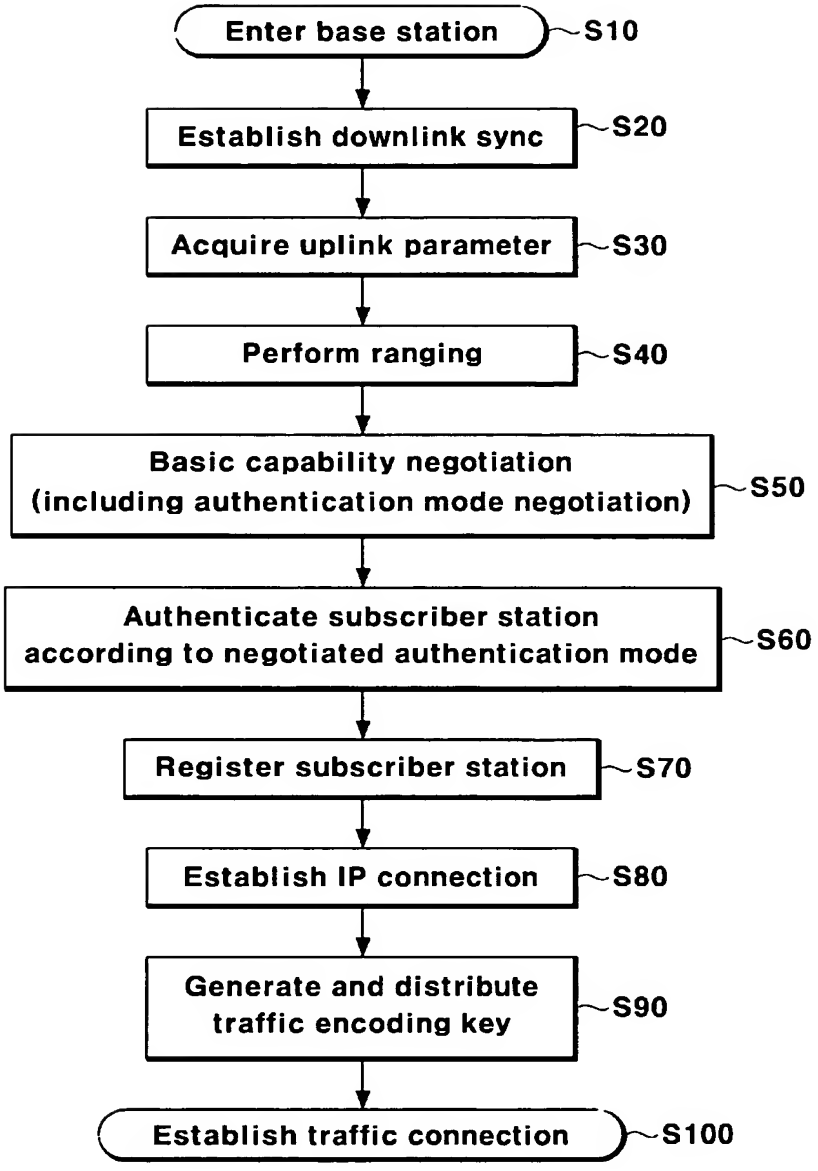
[Fig. 3]

FIG.3


Subscriber station
(SS)
Base station
(BS)
MAC
layer
Connection
C1
MAC
layer
Frame
Physical
layer
Physical
layer

[Fig. 4]

FIG.4


Enter base station
S10
Establish downlink sync
S20
Acquire uplink parameter
S30
Perform ranging
S40
Basic capability negotiation
(including authentication mode negotiation)
S50
Authenticate subscriber station
according to negotiated authentication mode
S60
Register subscriber station
S70
Establish IP connection
S80
Generate and distribute
traffic encoding key
S90
Establish traffic connection
S100

[Fig. 5]

FIG.5

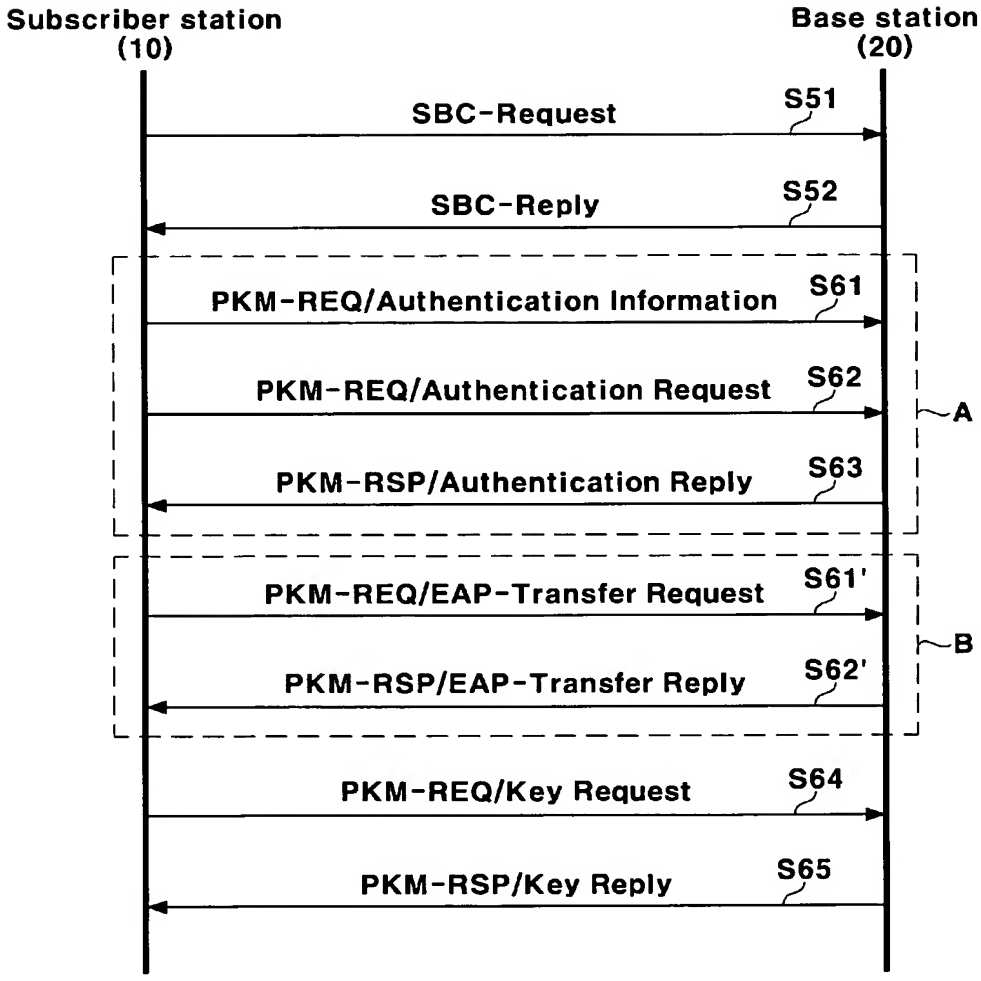
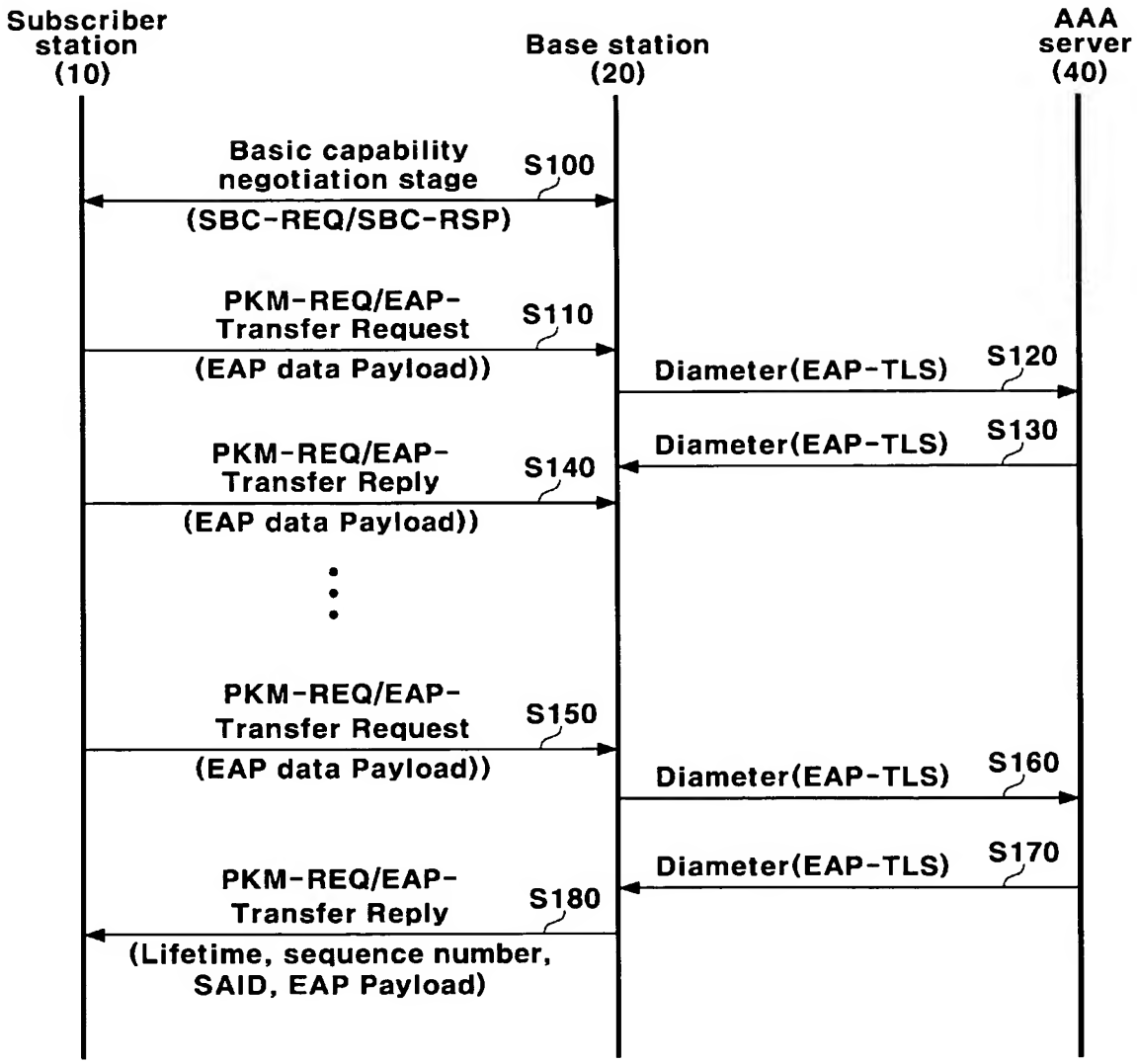

Subscriber station
(10)
Base station
(20)
SBC-Request
S51
SBC-Reply
S52
PKM-REQ/Authentication Information
S61
PKM-REQ/Authentication Request
S62
A
PKM-RSP/Authentication Reply
S63
PKM-REQ/EAP-Transfer Request
S61'
B
PKM-RSP/EAP-Transfer Reply
S62'
PKM-REQ/Key Request
S64
PKM-RSP/Key Reply
S65

FIG.6

Syntax	Size	Notes
SBC-REQ_Message_Format() {		
Management Message Type = 26	8 bits	
TLV Encoded Information {	Variable	TLV specific
Bandwidth Allocation Support	8 bits	Define by bitmap format
Authorization Policy Support	8 bits	Define by bitmap format
Physical Parameters Supported {		
Demodulator	8 bits	Bit#0 = 64-QAM Support
Modulator	8 bits	Bit#0 = 64-QAM Support
FFT Size	8 bits	Bit#1 = FFT-2048
}		
}		
}		

[Fig. 7]

FIG.7


Subscriber station (10)
Base station (20)
AAA server (40)
Basic capability negotiation stage
S100
(SBC-REQ/SBC-RSP)
PKM-REQ/EAP-Transfer Request
S110
(EAP data Payload))
Diameter(EAP-TLS)
S120
Diameter(EAP-TLS)
S130
PKM-REQ/EAP-Transfer Reply
S140
(EAP data Payload))
PKM-REQ/EAP-Transfer Request
S150
(EAP data Payload))
Diameter(EAP-TLS)
S160
Diameter(EAP-TLS)
S170
PKM-REQ/EAP-Transfer Reply
S180
(Lifetime, sequence number, SAID, EAP Payload)

[Fig. 8]

FIG.8

Code	PKM Message Type	MAC Message Type
0~2	Reserved	
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-REQ
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	EAP-transfer Request	PKM-REQ
14	EAP-transfer Reply	PKM-RSP
15~255	reserved	

[Fig. 9]

FIG.9

EAP transfer Request attributes

Attributes	Contents
Security-Capabilities	Describes requesting SS's security capabilities
SAID	SecurityAssociation ID, being equal to the Basic CID
EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

EAP transfer Reply attributes

Attributes	Contents
EAP Result Code	Describes success or failure
Authoriazation Action Code	Describes SS's policy, re-authorization or re-initialization
Key Sequence Number	Authorization Key sequence number
Key Life Time	Authorization Key life time
SA Descriptor	Specifies an SAID and additional properties of the SA
EAP Payload	Contains the EAP-TLS Data, not interpreted in the MAC

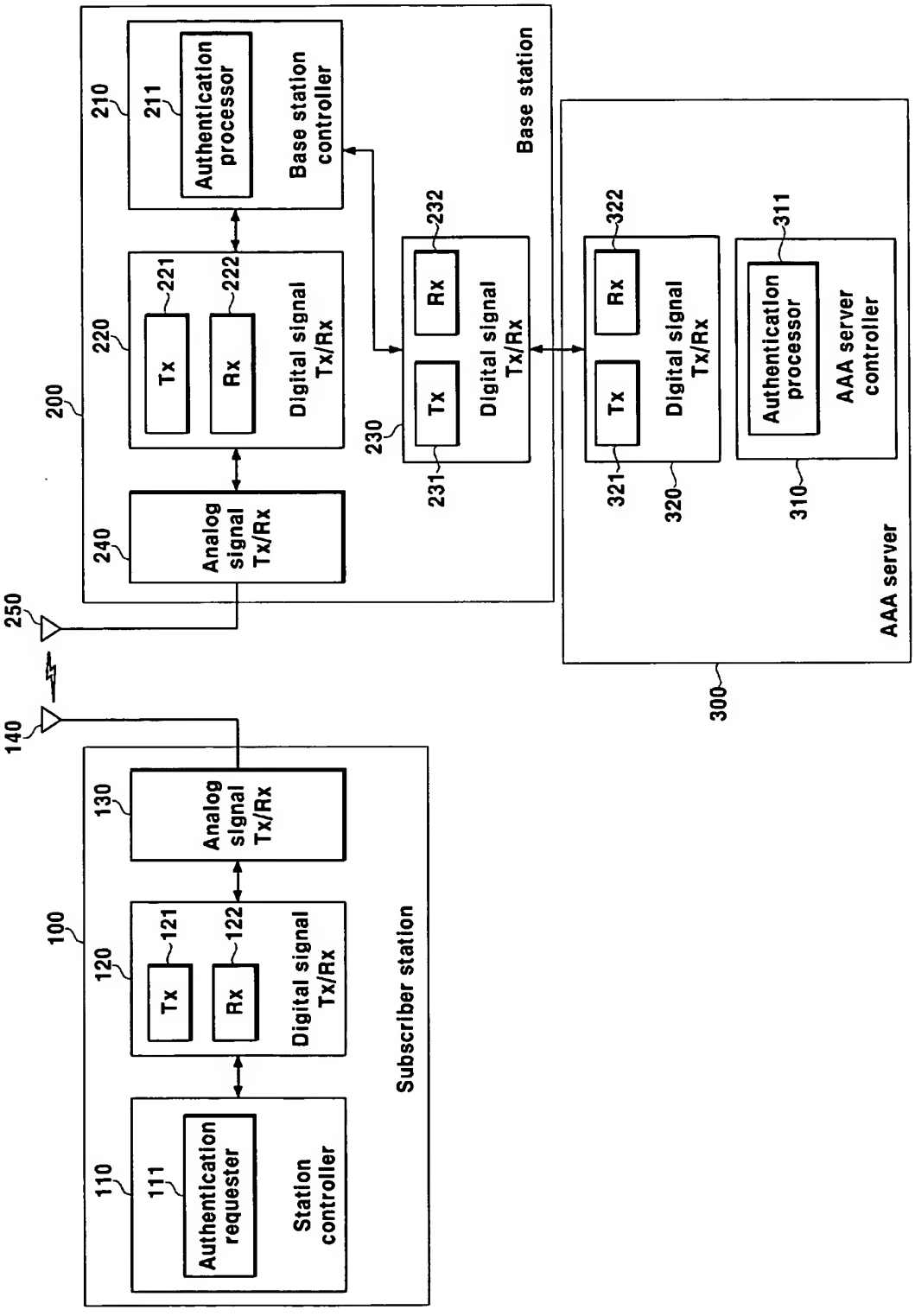
[Fig. 10]

FIG.10

Type	Length	Value	Scope
5.21	1	bit #0 : 802.16 Privacy - 701 bit # 1 : Open Privacy - 702 bit #2-7 : reserved; shall be set to zero - 703 (bit #2 : EAP-TLS, bit #3 : EAP-TTLS) - 704	SBC-REQ (see 1.1.1.1.1) SBC-RSP (see 1.1.1.1.2)

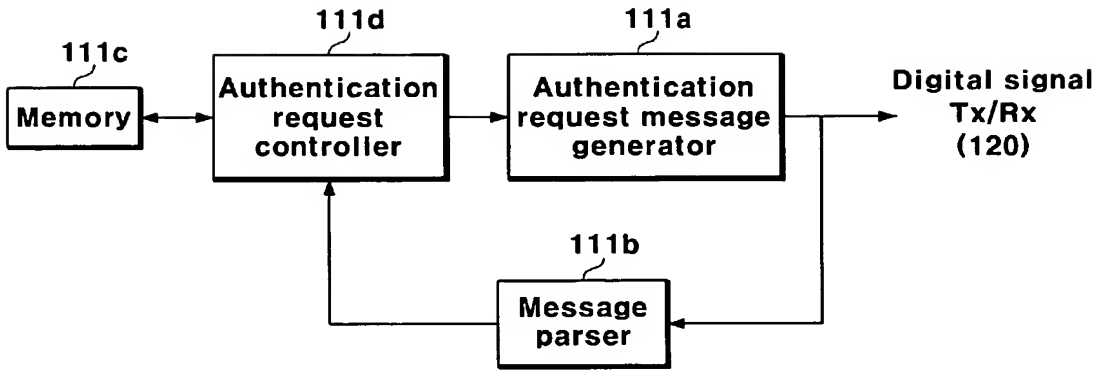
[Fig. 11]

FIG.11


Base station
200
210
211
Authentication processor
Base station controller
220
221
Tx
222
Rx
Digital signal Tx/Rx
240
Analog signal Tx/Rx
230
231
Tx
232
Rx
Digital signal Tx/Rx
250
140
AAA server
300
321
Tx
322
Rx
Digital signal Tx/Rx
320
310
311
Authentication processor
AAA server controller
Subscriber station
100
110
111
Authentication requester
Station controller
120
121
Tx
122
Rx
Digital signal Tx/Rx
130
Analog signal Tx/Rx

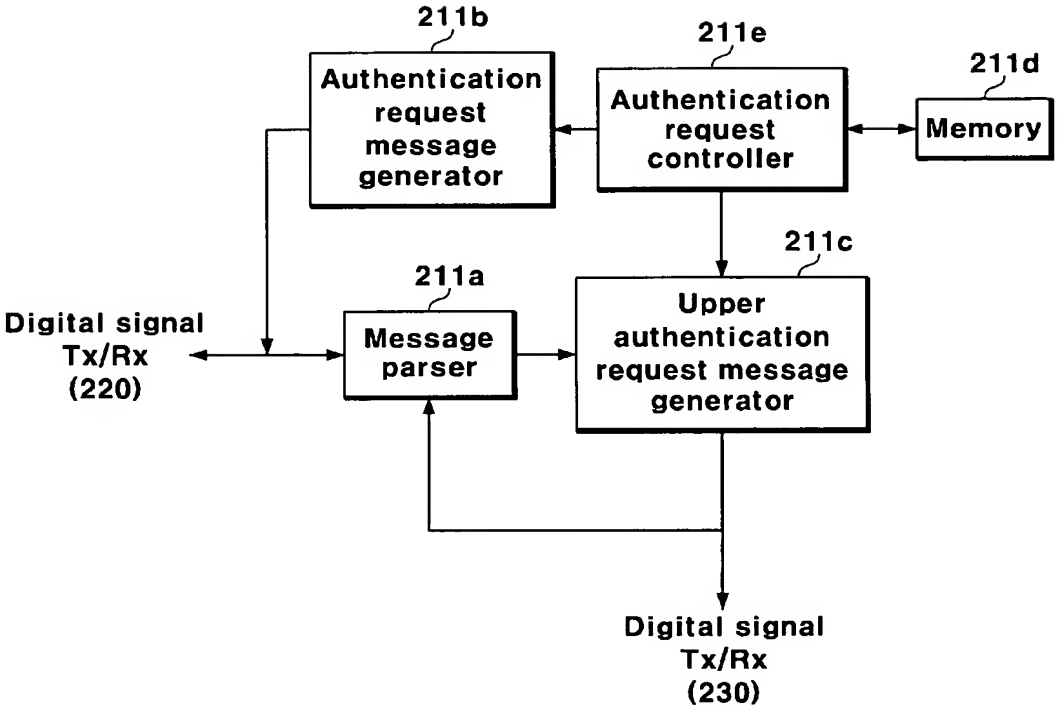
[Fig. 12]

FIG.12


111c
Memory
111d
Authentication request controller
111a
Authentication request message generator
Digital signal Tx/Rx (120)
111b
Message parser

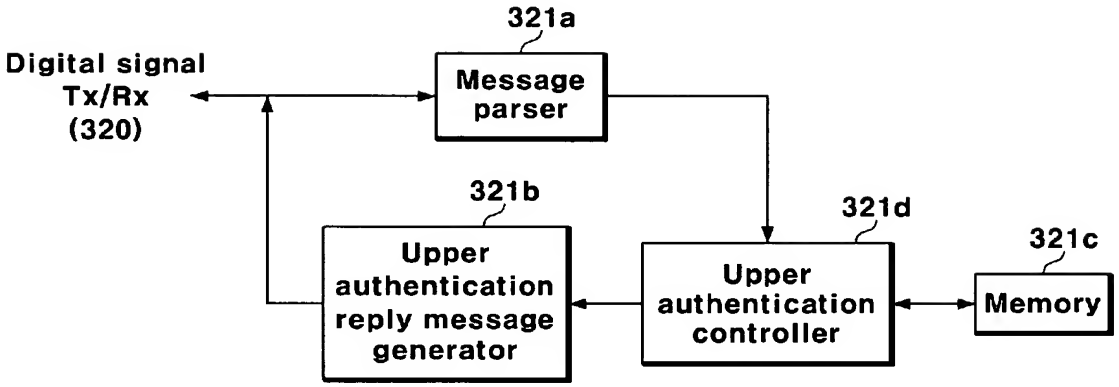
[Fig. 13]

FIG.13


211b
Authentication request message generator
211e
Authentication request controller
211d
Memory
211c
211a
Message parser
Upper authentication request message generator
Digital signal Tx/Rx (220)
Digital signal Tx/Rx (230)

[Fig. 14]

FIG.14


Digital signal
Tx/Rx
(320)
321a
Message parser
321b
Upper authentication reply message generator
321d
Upper authentication controller
321c
Memory